

Notes for Algebraic Structures

Spring 2016

Transcribed by Jacob Van Buren
(jvanbure@andrew.cmu.edu)

Notes for Algebraic Structures, taught Spring 2016 at Carnegie Mellon University, by Professor Clinton Conley.

Administrativa

Instructor. Clinton Conley (clintonc@andrew.cmu.edu), WEH 7121
<http://www.math.cmu.edu/~clintonc/>

Grading. 20% HW, $20\% \times 2$ midterms, 40% Final

Homework. Wednesday-Wednesday. Graded for completeness, one starred problem for which no collaboration of any type is allowed.
Most homework out of textbook (“D&F”).

Contents

Administrativa	
The Integers	1
Lecture 1 (2016-01-11)	1
Lecture 2 (2016-01-13)	1
Lecture 3 (2016-01-15)	2
The Integers (mod n)	3
Groups	5
Lecture 4 (2016-01-20)	5
Symmetric Groups	7
Lecture 5 (2016-01-25)	7
Lecture 6 (2016-01-27)	8
Subgroups	9
(Left) Coset equivalence	10
Lecture 7 (2016-01-29)	10
Lecture 8 (2016-02-01)	12
Normal Subgroups	12
Homomorphisms	14
Index	15

The Integers

Lecture 1 (2016–01–11)

NOTATION. $\mathbb{N} := \{1, 2, 3, \dots\}$ in this class.

Properties: Order, other things. Least element in a set S : $x \in S$ s.t. $\forall y \in S, x \leq y$
Addition $(\mathbb{Z}, +)$:

- Associativity $(x + y) + z = x + (y + z)$
- Identity $x + 0 = 0 + x = x$
- Inversion $x + (-x) = (-x) + x = 0$
- Commutativity $x + y = y + x$

Multiplication $(\mathbb{Z}, +, \cdot)$:

- Associative
- Distributive
- Identity (“1”)

Integer division: Assume x an integer and $y \in \mathbb{Z}^+$ then $\exists! d \in \mathbb{Z}, \exists! r \in \mathbb{Z} : 0 \leq r < y, x = d \cdot y + r$

DEFINITION 1. $y|x$ “ y divides x ” iff $\exists d \in \mathbb{Z} : x = d \cdot y$.

E.g. $3|9, 4 \nmid 7$.

DEFINITION 2. d is a gcd of x and y if

- $d|x, d|y$
- If $c|x$ and $c|y$ then $c|d$

Lecture 2 (2016–01–13)

DEFINITION 3. Given $a, b \in \mathbb{Z}$, denote by $\mathbb{Z}(a, b)$ the set $\{ax + by | x, y \in \mathbb{Z}\}$.

THEOREM 4 (Euclid, Bezout). Suppose $a, b \in \mathbb{Z}$ are nonzero and let d be the smallest positive element of $\mathbb{Z}(a, b)$, then d is the unique positive GCD of a and b .

PROOF. d is a gcd of a, b

(1) (Existence of positive GCD)

- (a) By integer division, $\exists q \in \mathbb{Z}, \exists r \in \mathbb{Z}$ with $0 \leq r < d$ such that $a = qd + r$. If $r = 0$ then $d|a$, so done. Otherwise, suppose $0 < r < d$, so $r = a - qd$ since $d \in \mathbb{Z}(a, b)$, we may fix x, y st $d = ax + by$, meaning $r = a - q(ax + by) = a(1 - qx) + b(-qy)$, so $r \in \mathbb{Z}(a, b)$, meaning d was not the minimal positive element in $\mathbb{Z}(a, b)$, RAA. Thus, $d|a$
- (b) HW: If $c|a$ and $c|b$ then $c|(ax + by)$ for all $x, y \in \mathbb{Z}$ Hence $c|d$

- (2) (Uniqueness of positive GCD) Suppose d_1, d_2 are both positive gcds of a and b . $d_1 | d_2$ and $d_2 | d_1$ as they are both gcds. i.e., $\exists m, n \in \mathbb{Z}$ such that $d_2 = md_1$ and $d_1 = nd_2$. As $\text{sgn}(d_1) = \text{sgn}(d_2)$, $m \geq 0$ and $n \geq 0$. As $d_1 = mnd_1$, $m = n = 1$. Thus $d_1 = d_2$. \square

DEFINITION 5. Relatively prime $\iff \gcd(a, b) = 1$

THEOREM 6. Suppose p is prime and $a, b \in \mathbb{Z}$ are nonzero, and $p | (ab)$ then $p | a$ or $p | b$.

PROOF. Consider $d = \gcd(p, a)$. Since $d | p$, we know $d = p$ or $d = 1$.

If $d = p$: By def of GCD, $d | p$ and $d | a$ ie. $p | p$ and $p | a$ so we're done.

If $d = 1$: Fix integers x and y such that $px + ay = 1$. $b = p(xb) + (ab)y$ as $p | p(xb)$ and $p | \underbrace{(ab)}_{\uparrow} y$, $p | b$. \square

THEOREM 7 (Unique Prime Factorization). Suppose that $a > 1$ an integer, $m, n \geq 1$ and $p_1 \leq p_2 \leq \dots \leq p_m, q_1 \leq q_2 \leq \dots \leq q_n$ are positive primes.

Then $m = n$ and $p_i = q_i$ for all i .

PROOF. By induction, it suffices to show $p_1 = q_1$. Suppose not. WLOG, assume $p_1 < q_1$. We know that $p_1 | a$ (as $p_1 | q_1 q_2 \dots q_n$) Hence, $\exists i \leq n$ such that $p_i | q_i$. since p_i and q_i prime, $p_i = q_i$. However, $p_1 < q_1 \leq q_i = p_1$ so $p_1 < p_2$ contradiction.

Hence $p_1 = q_1$ so by induction, we're done. \square

Lecture 3 (2016-01-15)

Teaser: Construct numbers of the form $a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$.

Notion of addition still exists: (similar to complex numbers, coefficients remain integers)

Same with multiplication

Among these "numbers", 2 is irreducible. But, 2 is not prime, as $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 + \sqrt{-5})$, but $2 | \underbrace{(1 + \sqrt{-5})(1 - \sqrt{-5})}_{=6=2 \cdot 3}$.

The Integers (mod n)

For today, $n > 0$.

DEFINITION 8. For $a, b \in \mathbb{Z}$ we say $a \equiv b \pmod{n}$ iff $n \mid (b - a)$.

\equiv is an *equivalence relation*

- Reflexivity: $a \equiv a$
- Symmetry: $a \equiv b \iff b \equiv a$
- Transitivity: $a \equiv b \wedge b \equiv c \implies a \equiv c$

PROOF. We know that $a \equiv b$ and $b \equiv c$, i.e. $n \mid (b - a)$ and $n \mid (c - b)$. We want $a \equiv c$, i.e., $n \mid (c - a)$

$$c - a = c + (-b + b) - a = \underbrace{(c - b) + (b - a)}_{n \text{ divides these}}$$

□

DEFINITION 9. Denote by \bar{a} or $[a]_n$ the equivalence class of a with respect to $\equiv \pmod{n}$ (I.e., The set $\{b \in \mathbb{Z} : a \equiv b \pmod{n}\} = \{a + kn : k \in \mathbb{Z}\}$).

EXAMPLE. If $n = 2$, there are 2 equivalence classes:

$$\bar{0} = \{\dots, -4, -2, 0, 2, 4, \dots\} = \bar{2} = \bar{-36}$$

$$\bar{1} = \{\dots, -3, -1, 1, 3, \dots\}$$

DEFINITION 10. Denote by $\mathbb{Z}/n\mathbb{Z}$ the collection of all $\equiv \pmod{n}$ equivalence classes.

E.g. $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$

“Define” addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ as follows:

$$\begin{aligned}\bar{a} + \bar{b} &= \overline{a + b} \\ \bar{a} \cdot \bar{b} &= \overline{ab}\end{aligned}$$

Makes sense, but we need to check that this definition makes any sense at all (make sure it's *well-defined*). Specifically, we need to make sure that the results of these operations doesn't depend on the representatives of the equivalence classes we chose (e.g. check that $\bar{x} + \bar{z} \equiv \bar{y} + \bar{z}$ if $x \equiv y$).

For brevity, we just show addition.

THEOREM 11. $+$ and \cdot are well-defined on $\mathbb{Z}/n\mathbb{Z}$

PROOF. (of \cdot) Assume that $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Then, we want to show that $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

We know: $n \mid (a_2 - a_1)$ and $n \mid (b_2 - b_1)$.

We want: $n \mid (a_2b_2 - a_1b_1)$.

$$\begin{aligned} a_2b_2 - a_1b_1 &= a_2b_2 + (-a_1b_2 + a_1b_2) - a_1b_1 \\ &= (a_2b_2 - a_1b_2) + (a_1b_2 - a_1b_1) \\ &= \underbrace{(a_2 - a_1)b_2 + a_1(b_2 - b_1)}_{n \text{ divides these}} \end{aligned}$$

So, $n \mid (a_2b_2 - a_1b_1)$ as desired □

Remark: This is a special case of a “quotient construction,” in which you start with a set and an equivalence relation on it and operations on the set that “respect” the equivalence relations (i.e. equivalent inputs yield equivalent outputs)

Moar notes: Multiplicative inverses are uncommon in the integers (only for 1 and -1). However, it’s “more prevalent” in $\mathbb{Z}/n\mathbb{Z}$ in the following sense:

THEOREM 12. *Suppose $n > 0$ is an integer, $a \in \mathbb{Z}$ such that $\gcd(n, a) = 1$ (they’re coprime). Then there is $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$ (alternatively, $\bar{a} \cdot \bar{b} = \bar{1}$)*

PROOF. Use Bezout’s theorem (from last lecture) Take integers x, y such that $nx + ay = \gcd(a, n) = 1$. Then, $nx = 1 - ay$, so $n \mid (1 - ay)$, so $1 \equiv ay \pmod{n}$. Choose $b = y$ and we’re done ($\bar{a}\bar{b} \equiv \bar{1}$). □

Groups

DEFINITION 13. We say that $*$ is a binary operation on some set X if it is a function $*$: $X \times X \rightarrow X$. (That is, $*$ accepts two (ordered) inputs from X and it outputs one element of X .)

Remark: usually write $a * b$ for the output of $*$ on the input (a, b) .

DEFINITION 14. A group is a set G with a binary operation $*$ (often abbreviated $(G, *)$) satisfying the following 3 axioms.

- i. Associativity: $\forall a, b, c \in G : (a * b) * c = a * (b * c)$
- ii. Identity: There is some $e \in G$ such that $\forall a \in G : a * e = e * a = a$
- iii. Inversion: $\forall a \in G (\exists b \in G (a * b = b * a = e))$ (where e is as described in ii)

Lecture 4 (2016–01–20)

Recall the definition of a group.

DEFINITION 15. $(G, *)$ is an abelian (commutative) group if it is a group and

- iv. $(G, *)$ is commutative ($\forall x, y \in G : x * y = y * x$)

Let $(G, *)$ be an arbitrary but fixed group.

PROPOSITION 16. *There is a unique identity element.*

PROOF. Suppose e and f both satisfy the second group property. we compute $e * f$ in two ways. $e * f = f$ and $e * f = e$, so by transitivity, $e = f$. □

PROPOSITION 17. *If $a \in G$, a has a unique inverse.*

PROOF. Suppose that b and c are both inverses for a , $b * a = e$, $a * c = e$. Then,

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c$$

□

Notational Conventions.

- We will often just call a group G instead of $(G, *)$
- We abbreviate multiplication $(x * y)$ as $x \cdot y$ or just xy
- We will often write xyz for $(x * y) * z$ (due to associativity)
- When working with $(\mathbb{Z}, +)$, we'll just use $+$
- We'll denote the (unique) identity of G by 1 or by e .
- We'll denote the inverse of x by x^{-1}
- Given an integer exponent $n \in \mathbb{Z}$ and $x \in G$, define

$$x^n = \begin{cases} \prod_{i=1}^n x, & \text{if } n > 0 \\ e, & \text{if } n = 0 \\ \prod_{i=1}^{-n} (x^{-1}), & \text{if } n < 0 \end{cases}$$

Group Examples. “Definition:” $\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}^+ \right\}$

- (1) $(\mathbb{Z}, +)$ is an abelian group
- (2) (\mathbb{Z}, \times) is not a group
Why? 2 has no inverse in \mathbb{Z} . ($\nexists x \in \mathbb{Z} : (2x = 1)$)
- (3) $(\mathbb{Q}, +)$ is an abelian group
- (4) (\mathbb{Q}, \times) is not a group (0 has no inverse)
- (5) $(\mathbb{Q} \setminus \{0\}, \times)$ is an abelian group.
- (6) $\text{GL}(n)$ is the set of matrices $A_{n \times n}$ for which $\det A_{n \times n} \neq 0$
- (7) The set G of 2×2 matrices with determinant 1, along with matrix multiplication, is a group. Called the “special linear group.”

Closure:

$$\det \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) = (bc - ad)(fg - eh) = 1$$

- i. Associativity: proof left for the reader.
 - ii. Identity: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
 - iii. Given $a = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, take $a^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, which you can verify is still in G .
- The group is *not* abelian. Take $a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Verify that $ab \neq ba$
- (8) Suppose that $X \neq \emptyset$ is some set, and denote by S_X the set of bijections $f : X \rightarrow X$. Then (S_X, \circ) is a group, where \circ is function composition. ($(f \circ g)$ is the function $x \mapsto f(g(x))$.)
- Identity is $x \mapsto x$. Inversion $f^{-1} = f^{-1}$.

Symmetric Groups

Lecture 5 (2016–01–25)

Recall: if X is a set then S_X is the group of bijections on it.

DEFINITION 18. S_X (or Sym_X) is called the symmetric group on X .

Note: \circ is associative because $(f \circ g) \circ h$ is

$$x \xrightarrow{h} (x) \xrightarrow{g} g(h(x)) \xrightarrow{f} f(g(h(x)))$$

Note: if $X = \{1, \dots, n\}$, then we usually write $\underline{S_n}$ instead of $S_{\{1, \dots, n\}}$. (Sometimes called symmetric group of degree n .)

Let's examine S_3 :

elt.	1	2	3
e	1	2	3
a	1	2	3
b	1	3	2
c	2	3	1
d	3	1	2
f	3	2	1

The group has $6 = 3!$ elements.

Lets compute ab and ba

$ab = a \circ b$, looking it up in the table gives $ab = d$ and $ba = c$.

In particular, S_3 is not abelian.

DEFINITION 19. A cycle is a permutation σ of the following form:

There is a sequence x_1, x_2, \dots, x_m of finitely many (distinct) elements of $\{1, 2, \dots, n\}$ such that $\sigma(x_{i-1}) = x_i$, $\sigma(x_m) = x_1$, and $\sigma(y) = y$, for $y \notin \{x_1, \dots, x_m\}$.

We call m the length of the cycle.

Ex. In S_3 , $d = \frac{1\ 2\ 3}{3\ 1\ 2}$ is a cycle of length 3, with $x_1 = 1, x_2 = 3, x_3 = 2$.

Ex. In S_3 , $a = \frac{1\ 2\ 3}{1\ 3\ 2}$ is a cycle of length 2, with $x_1 = 2, x_2 = 3$.

NOTATION. Given a cycle, we can efficiently denote it by $(x_1\ x_2\ x_3\ \dots\ x_m)$.

EXAMPLE. In S_3 , $a = \frac{1\ 2\ 3}{1\ 3\ 2}$ would be written as $(1\ 3\ 2)$.

Let's work in S_5 .

$\varphi := \frac{1\ 2\ 3\ 4\ 5}{3\ 4\ 1\ 5\ 2}$ is not a cycle, but it is the “superposition” of two cycles $(1\ 3)$ and $(2\ 4\ 5)$. Thus, we may write $\varphi = (1\ 3) \circ (2\ 4\ 5)$, or $(2\ 4\ 5)(1\ 3)$.

THEOREM 20. *Every permutation in S_n may be written as the product of “disjoint” cycles. (The identity is the empty product).*

PROOF. Sketch: If you have e then you're done trivially. Otherwise, fix the least element x of $\{1, \dots, n\}$ "moved" by σ (i.e. $\sigma(x) \neq x$). Look at $x, \sigma(x), \sigma^2(x), \dots, \sigma^m(x) = \sigma^n(x)$, $n < m$. So, as σ is invertible, $\sigma^{m-n}(x) = x$, so x is part of a cycle. \square

THEOREM 21. *Cycles can be written as a product of transpositions.*

General propositions on inversion in groups. Let G be a group, and let $a, b, x \in G$ be arbitrary.

- $(a^{-1})^{-1} = a$

PROOF. Show that a is the inverse of a^{-1} . Follows from group axiom. \square

- $(ab)^{-1} = b^{-1}a^{-1}$

PROOF. $(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$. Similarly, this works when we multiply from the other side. \square

Lecture 6 (2016-01-27)

DEFINITION 22. The cardinality (or order) of a group G is the number of elements in it, denoted by $|G|$.

EXAMPLE.

- $|\mathbb{Z}| = \infty (= \aleph_0)$
- $|\mathbb{Z}/5\mathbb{Z}| = 5$
- $|S_4| = 4! = 24$

DEFINITION 23. Given a group G and $x \in G$, the order of x is the smallest integer $n > 0$ such that $x^n = e$. If no such n exists, we say the order is ∞ .

We denote by $|x|$ the order of x .

EXAMPLE. In $(\mathbb{Z}, +)$: $|0| = 1$, $|5| = \infty$.

In S_5 : $|(1\ 3)| = 2$, $|(2\ 4\ 5)| = 3$, $|(1\ 3)(2\ 4\ 5)| = 6$.

PROPOSITION 24. *If G is a finite group, every $x \in G$ has finite order. Moreover, $|x| \leq |G|$.*

PROOF. Say $|G| = k$. Consider the sequence $x^0, x^1, x^2, \dots, x^k$. There are $k+1$ items in the sequence. So $\exists m < n$ such that $x^m = x^n$. $x^{n-m} = x^n x^{-m} = x^m x^{-m} = e$. As $0 < n - m \leq k$, it follows that $|x| \leq n - m \leq |G|$. \square

Subgroups

DEFINITION 25. Suppose $(G, *)$ is a group and $H \subseteq G$ some subset of G . We say H is a subgroup of G , written $H \leq G$ if $(H, *)$ happens to be a group, i.e., the following properties hold:

$*$ is a associative binary operator on H (i.e., it's closed) with inverses and an identity element.

EXAMPLE.

- $\mathbb{Z} \leq \mathbb{Q}$ (under addition)
- Even integers $\leq \mathbb{Z}$ (under addition)
- $n\mathbb{Z} \leq \mathbb{Z}$, where $n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$
 Aside: every subgroup of \mathbb{Z} is of the form $n\mathbb{Z}$
- $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \leq S_4$.

PROPOSITION 26. (HW): $H \leq G$ iff

- (a) $H \neq \emptyset$ (nonempty)
- (b) $\forall x, y \in H (xy \in H)$ (closed under product)
- (c) $\forall x \in H (x^{-1} \in H)$ (closed under inverses)

PROPOSITION 27. Suppose G is a finite group. Then $H \leq G$ iff $H \neq \emptyset$ and $\forall x, y \in H : xy \in H$.

PROOF. We show that for $H \subseteq G$ (a) and (b) \implies (c) (letters from proposition (26))
 Fix $x \in H$. Since G is finite, $|x|$ is finite (in G). Say $|x| = n > 0$ $x^n = \underbrace{x \cdot x \cdot \dots \cdot x}_{n \text{ times}} = e_G$.

Hence, $e_G \in H$.

Examine x^{n-1} .

$$x^{n-1} = \begin{cases} x^0 = e & \text{if } n = 1 \\ \underbrace{x \cdot x \cdot \dots \cdot x}_{n \text{ times}} & \text{if } n > 1 \end{cases}$$

But $x^{n-1} = x^{-1}$, since $x^{n-1}x = x^n = xx^{n-1} = e$. Thus, (c) holds for H . □

REMARK. $\mathbb{N} = \{0, 1, \dots\} \subseteq \mathbb{Z}$, but $\mathbb{N} \not\leq \mathbb{Z}$, despite satisfying (a) and (b).

(Left) Coset equivalence

Suppose G is a group and $H \leq G$ is a subgroup of G .

DEFINITION 28. We say $x \sim y \pmod{H}$ if $x^{-1}y \in H$.

PROPOSITION 29. $\sim \pmod{H}$ is an equivalence relation.

PROOF.

- Reflexivity ($x \sim x$):
 $x^{-1}x = e \in H$, so $x \sim x$.
- Symmetry ($x \sim y \implies y \sim x$):
 We know $x^{-1}y \in H$. H is closed under inversion, so $H \ni (x^{-1}y)^{-1} = (y^{-1}(x^{-1})^{-1}) = (y^{-1}x)$. Thus, $y \sim x$.
- Transitivity ($(x \sim y) \wedge (y \sim z) \implies (x \sim z)$):
 We know $x^{-1}y \in H$ and $y^{-1}z \in H$.
 Thus, $H \ni (x^{-1}y)(y^{-1}z) = x^{-1}ez = x^{-1}z$, so $x \sim z$.

□

Lecture 7 (2016–01–29)

G is a group. $H \leq G$ a fixed subgroup of G .

Given $x, y \in G$, $x \sim y \pmod{H}$ iff

$$x^{-1}y \in H.$$

Last time: we showed it was an equivalence relation.

What are the equivalence classes of $\sim \pmod{H}$? We examine

$$\begin{aligned} [x] &= \{y \in G : x \sim y \pmod{H}\} \\ &= \{y \in G : x^{-1}y \in H\} \\ &= \{y \in G : \exists h \in H (x^{-1}y = h)\} \\ &= \{y \in G : \exists h \in H (x(x^{-1}y) = xh)\} \\ &= \{y \in G : \exists h \in H (y = xh)\} \end{aligned}$$

So, $[x]$ is exactly the set

$$\{xh : h \in H\}.$$

NOTATION. We write xH to abbreviate the set $\{xh : h \in H\}$.

DEFINITION 30. The equivalence class xH is called the (left) coset of x with respect to H .

NOTATION. The cyclic subgroup of x is denoted by $\langle x \rangle$.

Examples:

- $G = (\mathbb{Z}, +)$, $H = n\mathbb{Z} = \text{multiples of } n$. So $H \leq G$. For $x \in \mathbb{Z}$, its coset is $\bar{x} = \{x + h : h \in n\mathbb{Z}\} = \{x + nk : k \in \mathbb{Z}\}$
- $G = S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ Take $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \leq S_3$ (the cyclic subgroup of $(1\ 2\ 3)$).

So what are the cosets? $eH = \{eh : h \in H\} = \{h : h \in H\} = H$. (In general, eH is always just H). (Even more generally, $xH = H$ whenever $x \in H$.)

Another coset is $(1\ 2)H$. Just compute $(1\ 2)h$ for each $h \in H$. Thus

$$(1\ 2)H = \left\{ \begin{array}{lll} (1\ 2) & e & = (1\ 2) \\ (1\ 2) & (1\ 2\ 3) & = (2\ 3) \\ (1\ 2) & (1\ 3\ 2) & = (1\ 3) \end{array} \right\} = \{(1\ 2), (2\ 3), (1\ 3)\}$$

We note that $(1\ 2)H = (2\ 3)H = (1\ 3)H$, as each of those are in $(1\ 2)H$.

- $G = S_3$, $K = \langle (1\ 3) \rangle = \{e, (1\ 3)\} \leq G$. Analyze cosets mod K .

Easy coset: $eK = K$.

For the next coset, choose $(1\ 2\ 3)K$

$$(1\ 2\ 3)K = \left\{ \begin{array}{lll} (1\ 2\ 3) & e & = (1\ 2\ 3) \\ (1\ 2\ 3) & (1\ 3) & = (2\ 3) \end{array} \right\} = \{(1\ 2\ 3), (2\ 3)\}$$

Next coset after that is $(1\ 2)K = \{(1\ 2), (1\ 3\ 2)\}$.

We note that the equivalence classes mod K partition S_3 , Although they are not all subgroups.

In the last two examples, it wasn't a coincidence that each coset was of the same cardinality.

PROPOSITION 31. *Suppose G is a group, $H \leq G$, and $x \in G$. Then $|xH| = |H|$.*

PROOF. We establish a bijection between H and xH .

Define $\varphi : H \rightarrow xH$, $\varphi(h) = xh$.

CLAIM (1). φ is surjective.

PROOF. Suppose $y \in xH$.

By definition of xH , $\exists h \in H$ such that $y = xh$. so $y = \varphi(h)$. □(C1)

CLAIM (2). φ is injective.

PROOF. Suppose $h_1, h_2 \in H$ such that $\varphi(h_1) = \varphi(h_2)$.

By definition of φ , we have $xh_1 = xh_2$. Since G is a group, x has an inverse x^{-1} .

Thus, $x^{-1}(xh_1) = x^{-1}(xh_2) \implies h_1 = h_2$ as desired. □(C2)

Thus φ is a bijection, meaning $|xH| = |H|$ as desired. □(Prop.)

THEOREM 32 (Lagrange). *Suppose that G is a finite group and $H \leq G$. Then $|H|$ divides $|G|$.*

PROOF. Left coset equivalence partitions G into k equivalence classes of size $|H|$.

Thus $|G| = k|H|$, as desired. □

COROLLARY 33. *Suppose that G is a finite group and $x \in G$. Then $|x|$ divides $|G|$.*

PROOF. Consider $\langle x \rangle$ (the cyclic subgroup generated by x). $\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$, where $|x| = n$. $|\langle x \rangle| = n$. Hence $n = |x|$ divides $|G|$. □

Lecture 8 (2016–02–01)

We go to the previous lecture for examples.

Consider $G = S_3$, $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \leq G$, $K = \langle (1\ 3) \rangle = \{e, (1\ 3)\} \leq G$.

DEFINITION 34. If G is a group and $H \leq G$, denote by G/H (G “mod” H) the collection of (left) cosets of H in G .

EXAMPLE.

- (a) $n\mathbb{Z} \leq \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$
- (b) $S_3/H = \{eH, (1\ 2)H\}$, $eH = H$, $(1\ 2)H = \{(1\ 2), (2\ 3), (1\ 3)\}$
- (c) $S_3/K = \{e, (1\ 3)\}, \{(1\ 2\ 3), 23\}, \{(1\ 2), (1\ 3\ 2)\}$

Normal Subgroups

Fundamental question: When is there “natural” group operation on G/H ? Prototype: $\mathbb{Z}/n\mathbb{Z}$, $\overline{x} + \overline{y} = \overline{x + y}$.

Natural Attempt:

$$(g_1H)(g_2H) \stackrel{?}{=} (g_1g_2)H.$$

This works fine for (b) in the sense that if $g_1H = g_2H$ and $k_1H = k_2H$ then $(g_1k_1)H = (g_2k_2)H$ (verification left to reader).

But it *doesn't* work for (c). e and $(1\ 3)$ both represent eK . But they give *different* cosets after multiplication by $(1\ 2\ 3)$.

- $e(1\ 2\ 3) = (1\ 2\ 3)$
- $(1\ 3)(1\ 2\ 3) = (1\ 2)$.

In general, what would we need to have, in order to have multiplication in G/H be “well-defined?”

We want: $\underbrace{x_1 \sim x_2}_{x_1^{-1}x_2=h \in H} \text{ and } \underbrace{y_1 \sim y_2}_{y_1^{-1}y_2=k \in H} \implies x_1y_1 \sim x_2y_2$. Thus, we want $(x_1y_1)^{-1}(x_2y_2) \in H$.

$$(x_1y_1)^{-1}(x_2y_2) = (y_1^{-1}x_1^{-1})(x_2y_2) = y_1^{-1}(x_1^{-1}x_2)y_1k = \underbrace{y_1^{-1}hy_1}_{\in H} \underbrace{k}_{\in H} \in H$$

This expression motivates the definition of a normal subgroup

DEFINITION 35. If G is a group, and $N \leq G$, we say N is normal if for all $n \in N$, and $g \in G$, we have $g^{-1}ng \in N$. We write this as $N \trianglelefteq G$.

REMARK. For fixed $g \in G$, the map for $x \in G$

$$x \mapsto g^{-1}xg$$

is called conjugation by g .

Thus, N is normal if it is stable under all conjugation.

THEOREM 36. Let G a group $H \leq G$. Then the following are equivalent:

- (I) $(g_1H)(g_2H) = (g_1g_2)H$ is a well-defined group operation on G/H .
- (II) $H \trianglelefteq G$.

$$(II) \implies (I). \quad x_1^{-1}x_2 = h, y_1^{-1}y_2 = k. \quad (\text{Exercise for the reader})$$

□

(I) \implies (II). Suppose $h \in H$ and $g \in H$ want $g^{-1}hg \in H$.

Note: $e \sim h$ since $e^{-1}h = h \in H$.

By (I), we have $(eg)H = (eH)(gH) = (hH)(gH) = (hg)H$.

So, $gH = (hg)H$, meaning $g \sim hg$, so $g^{-1}hg \in H$.

□(thm)

PROPOSITION 37. *If G is abelian, every subgroup is normal.*

PROOF. Fix $H \leq G$, $h \in H$, $g \in G$. Then $g^{-1}hg = g^{-1}gh = h \in H$.

□

PROPOSITION 38. $G \trianglelefteq G$ and $\{e\} \trianglelefteq G$.

PROOF. $g^{-1}hg \in G$ and $g^{-1}eg = g^{-1}g = e \in \{e\}$.

□

DEFINITION 39. For $A \subseteq G$, denote by $g^{-1}Ag$ the set $\{g^{-1}ag : a \in A\}$.
Called the conjugate of A by G .

REMARK. Thus, N is normal *iff* $N \leq G$ and $\forall g \in G : g^{-1}Ng \subseteq N$.

PROPOSITION 40. $N \trianglelefteq G \implies \forall g \in G : g^{-1}Ng = N$

PROOF. Fix $n \in N$. we want $n \in g^{-1}Ng$. (This shows $N \subseteq g^{-1}Ng$.)
We know by $N \trianglelefteq G$ that $m = (g^{-1})^{-1}n(g^{-1}) \in N$. Then $m = gng^{-1}$.

CLAIM. $g^{-1}mg = n$

PROOF. $g^{-1}(gng^{-1})g = \cancel{(g^{-1}g)}n\cancel{(g^{-1}g)} = n$

□(Claim)

□(Prop)

Homomorphisms

DEFINITION 41. Suppose G, H are groups and $\varphi : G \rightarrow H$ is a function. We say φ is a homomorphism if $\forall g_1, g_2 \in G : \varphi(g_1 *_{G} g_2) = \varphi(g_1) *_H \varphi(g_2)$.

DEFINITION 42. Suppose $\varphi : G \rightarrow H$ is a homomorphism. The Kernel of φ is $\text{Ker}(\varphi) = \{g \in G : \varphi(g) = e_H\} = \varphi^{-1}(\{e_H\})$.

PROPOSITION 43. *Suppose $\varphi : G \rightarrow H$ is a homomorphism between groups. Then $K = \text{Ker}(\varphi) \trianglelefteq G$.*

PROOF.

CLAIM (1). $K \neq \emptyset$. In fact, $e_G \in K$.

PROOF. We know that e_G is the unique element of G such that $\forall g \in G (e_G g = g e_g = g)$. So, $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G) \varphi(e_G) = \varphi(e_G)$ Multiplying both sides by $\varphi(e_G)^{-1} \in H$ So $\varphi(e_G) = e_H$. $\square(\text{C1})$

CLAIM (2). $\forall g \in G \varphi(g^{-1}) = (\varphi(g))^{-1}$

PROOF. $\varphi(g^{-1})\varphi(g) = \varphi(gg^{-1}) = \varphi(e_G) = e_H$ By symmetry, $\varphi(g)\varphi(g^{-1}) = e_H$ $\square(\text{C2})$
 $\square(\text{Prop.})$

Index

S_n , 7
(Left) Coset Of x With Respect To H , 10
Associative, 1
Associativity, 1
Commutativity, 1
Distributive, 1
Identity, 1
Integer Division, 1
Inversion, 1
Kernel, 14
Relatively Prime, 2
Abelian, 5
Binary Operation, 5
Cardinality, 8
Conjugation By g , 12
Cycle, 7
Equivalence Class, 3
Gcd, 1
Group, 5
Homomorphism, 14
Length, 7
Normal Subgroup, 12
Normal, 12
Order, 8
Subgroup, 9
Symmetric Group Of Degree n , 7
Symmetric Group, 7
The Conjugate Of A By G , 13